FORRESTER®

FOR: Security &
Risk Professionals

The 15 Most Important Questions To Ask Your Cloud Identity And Access Management Provider

by Andras Cser, April 5, 2013

KEY TAKEAWAYS

Cloud IAM Provides A Multitude Of Business And Operational Benefits

Cloud IAM solutions: 1) enable critical IAM services between on-premises and SaaS apps; 2) provide an automated IAM solution for legacy applications; 3) enable critical IAM services between user populations; 4) natively integrate with heterogeneous user stores; and 5) allow S&R pros to offload IAM to someone else.

Full-Featured IAM Solutions Provide Workflow And Attestation

Identity and access management is not just access management but also identity management, which includes processes such as access request submission and review, provisioning, and attestation. Future-proof your vendor selection by understanding workflow features and business user friendliness for the above.

External-Facing (Outside In) And Internal-User-Serving (Inside Out) IAM Will Merge

As more organizations realize that they need to serve the extended enterprise and their customers' IAM needs in a coherent and consistent manner, your cloud IAM solution should support customer, partner, and internal IAM needs.

The 15 Most Important Questions To Ask Your Cloud Identity And Access Management Provider

by Andras Cser
with Eve Maler, Stephanie Balaouras and Jessica McKee

WHY READ THIS REPORT

During the past three years, cloud-based identity and access management (IAM) solutions have become a viable and cost-effective alternative to on-premises, commercial off-the-shelf (COTS), or in-house IAM systems. However, cloud-based solutions bring their own risks and challenges, so to help security and risk (S&R) professionals select the right cloud offering, we identified the 15 most important questions and requirements that any enterprise considering a cloud IAM offering should include in their request for proposal (RFP) and vendor negotiations.

Table Of Contents

Notes & Resources

Forrester interviewed 10 vendor and user companies and used research from client inquiries.

Related Research Documents

Use Commercial IAM Solutions To Achieve More Than 100% ROI Over Manual Processes
October 1, 2012

Source Your Identity And Access Management Capabilities
September 27, 2012

The Forrester Wave™: Enterprise Cloud Identity And Access Management, Q3 2012
July 19, 2012

Navigate the Future Of Identity And Access Management
March 22, 2012

CLOUD IAM PROVIDES A MULTITUDE OF BUSINESS AND OPERATIONAL BENEFITS

During the past three years, Forrester has witnessed a dramatic increase in the importance of cloud IAM solutions. Why? Because they:

- **Enable critical IAM services between an enterprise's ecosystem of on-premises and SaaS apps.** Cloud IAM offerings started as simple log-in portals for SaaS applications but evolved into a set of services and capabilities that are far more sophisticated and important to the success of an enterprise's cloud strategy. Today, they also provide: 1) provisioning to on-premises applications, and 2) trusted broker services between user populations of partner companies. The latter is very important because it eliminates the need for companies to go through the tedious process of forging bilateral federation agreements; instead, they federate through the cloud IAM provider as a hub.

- **Provide automated IAM solutions for on-premises, legacy applications.** We all know the definition of legacy: "It works." There are a number of apps that enterprises cannot easily move to the cloud, such as mainframe applications, in-house-developed applications, and, sometimes, systems containing highly sensitive information. It's also likely that the enterprise will not sunset these applications any time soon, and in the meantime, S&R pros must still facilitate and automate IAM for these apps. Cloud IAM helps create, change, and modify users and their privileges for these applications.

- **Enable critical IAM services between an enterprise's ecosystem of user populations.** Today, enterprises need to understand and allow access to on-premises and SaaS applications for not just their own employees but also for contractors, contingent workers, business partners, and, in some cases, even customers. For most enterprises, providing temporary employees and partners with a corporate-owned laptop with a VPN client and a one-time password generator token is no longer sustainable from a cost and data security perspective — and it's certainly not a viable option for your customers. Cloud IAM promises easy, business-centric, delegated administration and provides access to your business partners and customers. Cloud IAM providers have already perfected workflows to do this so that you don't have to.

- **Natively integrate with many heterogeneous user stores.** Microsoft's Active Directory (AD) is losing its dominance as the only corporate user store. With many SaaS applications requiring a user store, AD is no longer the king of the hill when it comes to holding user security information. Managing user stores for internal workers while *not* managing user stores for business partners (but taking some kind of a token or using federation) has become the norm. While on-premises IAM products have reluctantly supported the above requirements, cloud IAM solutions need to satisfy them natively.

- **Allow S&R pros to offload IAM to someone else.** More organizations are realizing that they don't want to get into building and maintaining IAM solutions or if they already built these solutions they want to get out.[1] Many small and medium-size businesses (SMBs) know they can't afford to spend hundreds of thousands of dollars to hire experienced IAM pros for the care and feeding of an on-premises IAM system. Even large enterprises are considering eliminating on-premises IAM systems because of large licensing and support costs and long implementation times. When implemented correctly, cloud IAM should not require more than one full-time employee — a major savings for companies that want to automate IAM but don't want to build out and maintain their IAM systems.

FIFTEEN QUESTIONS TO ASK YOUR CLOUD IAM VENDOR

So you're considering making the leap to or expanding your investment in a cloud IAM solution. We've compiled the top 15 questions you should ask your provider before taking the leap or more tightly integrating your extended ecosystems of applications, users, and devices (see Figure 1).

No. 1: "How Exactly Is Your Solution Priced?"

IAM solution pricing has traditionally been more complex than other middleware pricing. Vendors often offer pricing options that depend on such factors as the number of users, connected systems, and cloud applications. Forrester usually sees prices range from $1 to $4 per user per month for SMBs; enterprises will likely obtain volume discounts. Forrester expects that companies with 1,000 to 10,000 users will find the cloud IAM solution's pricing most attractive. Organizations with fewer than 1,000 users find that it makes financial sense to keep managing IAM manually, and organizations with more than 10,000 users find that implementing an on-premises IAM solution is less expensive — especially if they've already implemented some IAM functionality on-premises. For organizations with 1,000 to 10,000 users, cloud IAM solutions are attractive because: 1) it makes sense to automate IAM, and 2) it's cost-prohibitive to hire IAM maintenance personnel and licenses for an on-premises IAM solution.

Vendors with cloud IAM solutions often use a commercial off-the-shelf (COTS) IAM product as the foundation for their solution. In this situation, you will need to know if you pay upfront for the product licenses and maintenance or if the subscription includes the amortized license cost of the software licenses. For pure cloud-based solutions, you definitely need to have a full understanding of the pricing structure and mechanics and obtain a detailed pricing list in order to compare various cloud IAM providers' offerings. Leading vendors provide a trial period for the service as well. Common pricing schemes include a per-user per-month fee with an additional per-application fee. Forrester expects that vendors will soon provide per-transaction pricing. You can't take for granted that a cloud IAM solution will be less expensive than an on-premises approach; you must calculate the total cost of ownership for your solution using at least a three-to-five-year period.[2]

No. 2: "How Can You Help Me Move Between On-Premises And Cloud IAM Solutions?"

Making the decision to move to a cloud IAM solution will depend not only on how well you can segregate your user repositories but also on whether the provider supports your existing authoritative user sources such as PeopleSoft, Lawson, and Oracle on-premises human resources applications, or cloud-based like Workday and salesforce.com; and other contractor databases. Read/write connectivity to your existing AD user stores is a must. It's also imperative that the provider offer a detailed methodology that describes how to move your IAM capabilities to and from the cloud. Many organizations we talk with want to be sure they can leave the cloud IAM provider and bring IAM services back on-site when they need to.

Integration or replacement of legacy IAM solutions should be a two-way street. Forrester believes that adoption of cloud IAM solutions will hinge on how well they can integrate and consolidate the user stores of on-premises and cloud SaaS applications into a cloud user store, which can then drive provisioning into endpoints such as AD, LDAP, salesforce.com, and Workday. The ability to re-use your existing physical or logical one-time password token infrastructure is also often a requirement.

No. 3: "How Can Your Workflow Support My Business Processes?"

An IAM system is an imprint of your company's process DNA: It needs to map easily to your user joiner, mover, and leaver processes; requesting and reviewing applications and data access; and also your attestation processes. While you should always push for more business process simplification and standardization, at some point, the provider's solution needs to hit the ground running. A thorough understanding of what the provider's workflow can and cannot do to support your processes is critical. Many companies we interviewed noted that the provider's ability to expose the workflow as an API or web service was very important for seamless implementation. Obtain a written answer from the provider about the process of creating and maintaining custom IAM workflows; the provider must also clearly identify the owner of this intellectual property — before you select the provider. Forrester expects that vendors in the space will work on separating business workflow APIs from the presentation layer to allow for easier customization and faster time and thus lower cost-to-value.

No. 4: "How Can You Support My On-Premises Business Applications?"

Take an inventory of your internal systems that have IAM requirements, such as access control, access request management, attestation, and role management. Then determine which of these applications your IT organization will not sunset for the next 12 to 24 months. This is important because it means that you will have to continue to support them with IAM capabilities. Focus not just on access control but also on governance and provisioning. Moving forward, it will make less and less sense to use a cloud IAM system for access but an on-premises COTS solution for access governance or provisioning. In this case, ask the vendor for a single-pane-of-glass view of your applications. The cloud IAM providers should be able to provide all this, along with detailed pricing schedules and process descriptions on how they support provisioning connector development and maintenance.

No. 5: "How Easily Can You Support My SaaS Business Applications?"

Chances are that moving to cloud IAM is part of a broader cloud IT strategy at your company. Once you understand which SaaS applications need IAM support, you can obtain confirmation from your cloud IAM provider that it can integrate your SaaS apps into its cloud offering out-of-the-box and with minimal configuration or customization. In addition, ask for tested SaaS connectors (don't be satisfied with stock vendor answers such as "We do SAML and it should all work out OK"). This integration should include not just access control (single sign-on), but also federation, user account provisioning, access request management, reporting, and attestation.

No. 6: "How Do You Ensure The Confidentiality, Integrity, And Availability Of My Data?"

Clients have many questions regarding data mobility between their on-premises location and the provider's data centers.[3] Common questions include: "Who moves the data? Who is responsible for data security in flight and at rest, data backup, and how does the provider ensure that they don't share my data (even inadvertently) with the client's competitors who are also customers?" Forrester's customers prefer providers that own their own data centers (CA Technologies for example) and who have strong, documented, and verifiable access controls for both staff and contractors. S&R pros should pay attention to SLAs and demand that the provider compensate them somehow (refunds, etc.) for missing service-level agreements (SLAs). Performance is also very important: The provider must have enough capacity to ensure that there is no performance degradation during peak usage hours.

No. 7: "How Do You Help Me Comply With International Privacy Laws?"

To adopt cloud services, enterprises must understand the patchwork of often conflicting global data privacy laws. Countries enact these laws to protect an individual's personally identifiable information (PII) from abuse and theft.[4] Many of the privacy laws in Europe prohibit the transport of PII beyond country borders. However, there are ways to abide by privacy laws while still adopting cloud services. To do this, a cloud provider has a few options. It can: 1) ensure through automated policy that specific PII does not leave a given geography; 2) encrypt PII in flight and at rest; or 3) certify with the Safe Harbor Principles to process EU PII. Not surprisingly, many clients grill their cloud IAM providers about policies for data storage geographic location, data encryption (both in flight and at rest), and data segregation (are hard disks shared or specific to customers?).

No. 8: "What Certifications Do You Have? What Regulations Do You Comply With?"

There are several reasons for demanding to know what certifications a cloud provider has and with which industry or government regulations it must comply. First, security certifications such as ISO 27001 are good indicators that the provider has a baseline of security maturity. Second, if a provider has achieved certification under, say, the Federal Information Security Management Act (FISMA) and you are also subject to the same regulation, it can help address legal and compliance barriers to adoption. S&R pros routinely ask cloud IAM providers about SAS 70 and the SSAE 16 SOC 2

Report.[5] They want to know if the provider can demonstrate compliance with standards such as ISO 27001, PCI DSS, FISMA, or HIPAA. Government and public service customers we interviewed preferred providers to be Common Criteria certified. Firms also desired to see independent audits that prove that the vendor's solution source code is free of malicious code, back-doors, or other surreptitious logic.

No. 9: "What Protocols And Versions Do You Support Or Plan To Support, And When?"

Standards-based protocols are the backbone of secure, standardized, and inexpensive IAM — especially with mobile device native applications saying good-by to HTTP/S protocols and increasingly using REST-based APIs and OAuth. While there are many emerging protocols, you should make sure that your cloud IAM provider supports at least the following: 1) SAML 1.1 and 2.0, OpenID Connect (or at least the vendor's strategy for future support) for authentication; 2) OAuth, Duo Security, Google Authenticator for two-factor authentication; 3) OAuth for authorization if you have mobile application needs; 4) Simple Cloud Identity Management (SCIM) and comma separated values (CSV) files for user provisioning; and 5) any legacy secure token services (such as SiteMinder and Oracle Access Manager).[6] If the provider currently does not support a protocol you need, get a commitment in writing for when it will and provisions for the vendor ever missing a planned support date.

No. 10: "How Do You Support Different User Devices And Mobility?"

Part of the premise of cloud computing is that users can access services from anywhere at any time.[7] The same should apply to IAM. The cloud provider should support a broad array of web browsers and mobile device operating systems and should have at least native iOS and Android applications or APIs for submitting and reviewing access requests and performing simple attestation and two-factor authentication from mobile devices. Many vendors support mobile OS-based native application connectivity as well as mobile device-based applications, which aggregate all icons of SaaS applications you can access.

No. 11: "Will You Share Your Road Maps With Us?"

Since cloud IAM is a nascent and quickly evolving market, S&R pros have come to expect that vendors in this space will provide clients with predictable and transparent road maps and release cycles in order to allay fears and concerns. Our clients also tell us that they ask their cloud IAM provider about release cycle frequency. They also want to know how the provider releases new features; for example, are all of the provider's clients on the same code base, or is there some staggered release scheme?

No. 12: "How Fast Can You Respond To Incidents And Technical Support Issues?"

No provider is perfect or immune from natural disasters, IT failures, human error, disgruntled employees, or cyberthreats, so it's critical that as part of your vendor evaluation you understand the provider's incident response and technical support processes. We hear clients ask the following questions: "How do you handle incident management? Do you have SLAs regarding response and resolution to incidents? How do you deliver customer support (e.g., telephone, email, etc.)? Is support unlimited or charged? What has been your historical uptime during the past 12 months? How do you measure uptime?"

No. 13: "Who Staffs Your Data Centers, Technical Support, And Operations?"

At the end of the day, a solution is only as secure as the people who operate it.[8] We routinely hear clients ask the following questions: "Who handles security operations for your offering? Are they internal employees or do you use contractors? What processes do you use to vet employees and contractors who may have access to the environment and customer data?" On a more technical note, some clients also want to know how admin passwords expire and want to understand the provider's password policies.[9] Forrester recommends that, at a minimum, S&R pros make sure that the cloud IAM provider has adequate controls for privileged identity management, such as password check-outs from a password vault and session-recording, using an automated solution at the vendor's data center.

No. 14: "Whose IP Is It Anyway?"

Many cloud IAM providers are small companies, so clients are rightfully concerned about their financial stability and future. At a minimum, you need to understand the future of the provider's intellectual property (IP) in case the provider goes out of business.[10] Clients routinely ask for non-exclusive rights to the IAM provider's IP if that happens, and you should, too.[11]

No. 15: "How Do I Future-Proof My Cloud IAM Investment?"

Unlike outsourcing contracts of the past, cloud service contracts are far more flexible, are shorter in duration, and are based on pay-per-use pricing. However, it's still an investment of money and time, and in the case of IAM, there is a lot of integration. As with any investment, you want to ensure that it can meet future business and IT requirements. We hear customers ask about the following future requirements:

- **Risk-based authentication (RBA) with device fingerprinting.** Companies have long been using on-premises RBA coupled with device fingerprinting to reduce the burden of two-factor authentication for transactions where a user or customer is coming from a known low-risk location, such as a corporate office, in a low-risk geography, such as North America or Western Europe, from a previously seen device, such as their desktop PC or laptop.[12] Now cloud IAM providers are increasingly looking at either building these services themselves or partnering with RBA vendors.

- **Support for the company's customer-facing and business partner-facing applications.** After a successful implementation for internal enterprise users such as employees and contractors, companies often want to implement inbound identity and access management on their Internet portals and mobile applications for customers — to lower cost of customer-facing IAM.

- **Social log-in to eliminate password management.** For lower-risk transactions, such as reserving an appointment with a city council member, organizations have been using social log-in (Facebook Connect, Twitter, LinkedIn, etc.) with on-premises web access management platforms. We now see the same requirement for cloud IAM providers' solutions as well as for business partner and internal user authentication.

- **Lightweight user vetting and proofing.** Since cloud IAM providers serve hundreds of clients and increasing numbers of consumers, Forrester expects that, to compete with traditional out-of-wallet question-based user vetting sources such as Equifax, Lexis-Nexis, and Experian, they will provide lighter-weight identity verification or proofing services based on transaction information or social media. Example lightweight identity-proofing may include such questions as "Who of the following five individuals is not a friend of yours on Facebook?"

- **B2B federation broker services.** If users of two companies need to access each other's applications and both are clients of a cloud IAM provider, the cloud IAM provider can act as a federation hub (similar to Covisint, a Compuware Company; Exostar; and SAFE-Biopharma) to broker trust between its clients. This greatly reduces the need to form bilateral federation agreements and helps tremendously with setting up the legal framework for federation — something that has traditionally been problematic for many firms.

Figure 1 The 15 Most Important Questions To Ask Your Cloud IAM Provider

Major question	Subquestions
1. How exactly is your solution priced?	a) Do you fully disclose pricing? b) Is it priced based on users, active user applications, transactions? How? c) Is it a volume discount? d) Is there a multi-year agreement discount?
2. How can you help me move between on-premises and cloud IAM solutions?	a) What cloud HR systems are supported? b) What types of on-premises user stores are supported (AD, LDAP, SQL)? c) Can the solution provide an aggregated cloud user store with meta/ virtual directory views of all my users' rights? d) How can I move between on-premises IAM installations and licenses and your platform? e) Does the cloud IAM solution interoperate with a legacy on-premises Web SSO or provisioning system like SiteMinder or Quest One Identity Manager?
3. How can your workflow support my business processes?	a) What kind of provisioning does the cloud IAM solution support? b) How does the cloud IAM solution support attestation and role-based access control? c) How separate is the business logic from the user interface? d) How easy is the solution to customize to map to my business processes? e) How can you support access request management processes? f) How can you support delegated administration for business partners and multi-tenancy?
4. How can you support my on-premises business applications?	a) Specifically which on-premises solutions can the cloud IAM system provision? b) What versions? c) Is there an extra cost for this? d) What kinds of on-premises or cloud connectors do I have to install for this functionality?
5. How easily can you support my SaaS business applications?	a) Which SaaS applications are pre-integrated? b) Does the solution use SAML for integration, or does it use a lower security HTTP post? c) How can the cloud IAM solution provision into SaaS applications?
6. How do you ensure the confidentiality, integrity, and availability of my data?	a) Who is responsible for data security in flight and at rest, backups, and BC/DR? b) Who owns your data centers? c) What happens if you miss SLAs? Is there a refund? d) How do you make sure that you provide enough capacity and performance during peak usage (especially for B2C use)?
7. How do you help me comply with international privacy laws?	a) Where does my data physically reside? b) How do you make sure that my data does not leave the data center where it resides to a different country? c) How is data encrypted? d) Are you EU PII regulations compliant?
8. What certifications do you have? What regulations do you comply with?	a) Are you certified for ISO 27001? FISMA? b) Can you show me a recent SAS 70 and SSAE 16 SOC 2 Report? c) How can you demonstrate PCI DSS, FISMA, FERC/NERC, HIPAA, Common Criteria, or other relevant regulatory compliance?

94222 Source: Forrester Research, Inc.

Figure 1 The 15 Most Important Questions To Ask Your Cloud IAM Provider (Cont.)

Major question	Subquestions
9. What protocols and versions do you support or plan to support, and when?	a) SAML 1.1, 2.0? Inbound (IdP proxy)? b) OAuth? c) OpenID Connect? d) OpenID? e) OATH or Google Authenticator? f) SCIM? g) Secure Token Service (SiteMinder, OAM., etc.)? h) Other APIs? i) If the above is not there, when will it be?
10. How do you support different user devices and mobility?	a) Is there a mobile application portal for SaaS and on-premises applications? b) How is iOS supported as a client for single sign-on? c) How is Android supported as a client for single sign-on? d) How is Windows Phone supported as a client for single sign-on?
11. Will you share your road maps with us?	a) How often do I get a road map update? b) How can I influence the road map? c) How frequently do you release a new version? d) Are all of your clients on the same code base or is there some staggered release scheme?
12. How fast can you respond to incidents and technical support issues?	a) What types of incident response processes do you have? b) How do you measure uptime? c) What kind of SLA is there for responding to incidents? d) How do you make sure that if client A is attacked, client B is not impacted by a DDOS attack?
13. Who staffs your data centers, technical support, and operations?	a) Who handles security operations, provider contractors, or employees? b) What kinds of background checks do you have in place? c) What kinds of privileged identity management (PIM) processes and tools do you implement in your data center?
14. Whose IP is it anyway?	a) What happens to our data if you go out of business? b) What happens to your solution code base if you go out of business?
15. How do you future-proof my cloud IAM investment?	a) Do you support or plan to support Risk Based Authentication (RBA) with device fingerprinting? b) How can you support inbound customer and business partner portals? c) How do you support social log-in (Facebook Connect, etc.)? d) How do you support lightweight user vetting and proofing? e) How can you support B2B federation broker services?

94222 Source: Forrester Research, Inc.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Report

Aveksa
CA
Lighthouse Security Group
Okta
OneLogin
SailPoint Technologies
salesforce.com
Simeio Solutions
Symplified
Verizon

ENDNOTES

[1] In Forrester's 15-criteria evaluation of the emerging managed security services provider (MSSP) market, we identified the 10 most significant providers in this category — Alert Logic; CompuCom; Integralis; Network Box; Savvis, A CenturyLink Company; Secure Designs; SilverSky; StillSecure; Tata Communications; and Vigilant — and researched, analyzed, and scored them. See the January 8, 2013, "The Forrester Wave™: Emerging Managed Security Service Providers, Q1 2013" report.

[2] S&R pros can carry out identity and access management (IAM) processes using a combination of the following scenarios: 1) a manual IAM process; 2) a build-your-own on-premises IAM system; 3) a commercial off-the-shelf (COTS) on-premises IAM solution; and 4) a cloud-based IAM solution. This report and the accompanying tool help S&R executives quantify the cost and benefits for each of the scenarios to determine which one provides the best return on investment (ROI). See the October 1, 2012, "Use Commercial IAM Solutions To Achieve More Than 100% ROI Over Manual Processes" report.

[3] For more detailed guidance on general cloud security, see the October 29, 2010, "Q&A: Demystifying Cloud Security" report, see the May 18, 2012, "Put Guardrails In Place To Drive Cloud Success" report, and see the November 9, 2011, "Stop Ignoring Third-Party Risk" report.

[4] To help security and risk professionals navigate the complex landscape of privacy laws around the world, Forrester created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. See the December 22, 2011, "Introducing Forrester's Data Privacy Heat Map" report.

[5] When used for information security certification, CISOs routinely derided SAS 70 as "proving nothing." In response to this and other issues, the AICPA introduced new audit standards to replace SAS 70. This report provides insight to CISOs on these new audit standards and their effectiveness in auditing service providers for information security compliance. See the October 31, 2011, "SAS 70 Out, New Service Organization Control Reports In" report.

[6] IAM protocols are the building blocks of a non-web oriented IAM framework. For a detailed list of further IAM protocols, see the October 24, 2012, "TechRadar™ For Security Pros: Zero Trust Identity Standards, Q3 2012" report.

For provisioning into applications using standards, please see the July 15, 2011, "Understanding Simple Cloud Identity Management" report.

[7] The mobile market is evolving rapidly. Both the consumer and enterprise markets are experiencing major changes. Room exists for new innovations as well as for established players to develop new revenue opportunities. What challenges will various players in the mobile ecosystem face in the near future, and what opportunities will the market present to them? In this report, Forrester looks at current market and technology adoption trends and makes its mobile security predictions. See the March 26, 2013, "2013 Forrester Mobile Security Predictions" report.

[8] Third-party exclusions are an issue with all cloud SaaS providers. The vendor may develop the application but use AWS as its infrastructure. The contract with your vendor may not have sufficient indemnification for downstream providers.

[9] An identity and access management (IAM) maturity model is necessary for assessing your current state against industry best practices, understanding your performance relative to that of your peers, and creating a long-term strategy and road map. To help kick-start your IAM assessment, see the September 26, 2012, "Assess Your Identity And Access Management Maturity" report.

[10] While deal-specific risk mitigation should already be part of every SVM team's approach, expanding to a broader vendor risk management approach will require that the SVM reach out and build internal relationships and processes with colleagues in finance, enterprise risk, internal audit, and security. Risk professionals in particular can help you establish a formal vendor risk management program using existing risk management processes, taxonomies, tools, and other resources. For more specifics, see the January 10, 2011, "Building An Effective Vendor Risk Plan For Emerging Technology Suppliers" report.

[11] As with other SaaS services, code escrow and other techniques to insure supplier viability are critical. Engaging sourcing and vendor management is also important to make sure any corporate legal requirements are met.

[12] For a complete description of the six key vendors in the risk-based authentication market, see the February 22, 2012, "The Forrester Wave™: Risk-Based Authentication, Q1 2012" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On
Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals